Exhibit 6

Declaration of Mary Frantz

In re: Equifax Inc. Customer Data Security Breach Litigation,
No. 17-md-2800-TWT (N.D. Ga.)

Plaintiffs' Motion to Direct Notice of Proposed Settlement

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

IN RE:	)	
	)	**Case No.: 1:17-md-02800-TWT**
Equifax, Inc., Customer Data	)	
Security Breach Litigation	)	**Consumer Actions**
	)	
	)	

Declaration of Mary T. Frantz

I, Mary T. Frantz, pursuant to 28 U.S.C. § 1746, hereby declare as follows,

I. INTRODUCTION

1. Shortly after the commencement of this case, I was retained by counsel for the Consumer Plaintiffs to advise on the business practice changes needed to address the cyber security deficiencies in Equifax's systems and to assist in negotiating those changes in connection with any potential resolution of the Consumer Plaintiffs' claims.

2. I have been asked to consider whether the business practice changes proposed in Exhibit B to the Settlement Agreement, if approved, would provide a meaningful benefit to Consumer Plaintiffs', the classes they seek to represent, and other parties whose information Equifax collects, processes, or stores. In addition, I have been asked to evaluate if the proposed changes would meaningfully improve Equifax's overall security posture and remediate the deficiencies that enabled the data breach Equifax announced in 2017.

3. My opinions are based on my formal education and training, my review and assessment of information provided by Equifax and Consumer Plaintiffs' Counsel, generally accepted sources within the field of information security, and my nearly 30 years' of professional experience in cyber security, information technology, and compliance.

4. In my opinion, the business practice changes included in the proposed Settlement Agreement address the technical and administrative deficiencies that contributed to the Equifax data breach and would meaningfully reduce the risk of Equifax suffering another data breach during the settlement term. As such, the proposed business practice changes would confer a substantial benefit to the Class Members and all other stakeholders.

II. BACKGROUND AND QUALIFICATIONS

5. I am the Founder and Managing Partner of Enterprise Knowledge Partners, LLC (EKP) in Edina, Minnesota. EKP is a technology services firm specializing in eDiscovery, Forensics, Cyber Security and Enterprise Architecture. As a Managing Partner of EKP, I have provided a wide range of technology, compliance, and data security services to corporate clients.

6. My educational credentials include four Bachelor's degrees from Northern Illinois University in the following fields: Mathematics, Information Systems, International Relations, and Foreign Translation of Spanish, with a minor in French. In addition, I hold a Master's Degree in Business Administration from the University of Chicago (with emphasis on International Business Investment/Marketing). I also hold a Master's Degree in Engineering from the Georgia Institute of Technology (with emphasis on Computer Science Engineering). A copy of my resume is attached as Exhibit

A, which further details my education, professional experience, and expertise.

7. I hold multiple active and non-active certifications in information systems, data security, and technology architecture. I hold active certifications as a Certified Information Systems Auditor (CISA), Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), Certified Forensics Investigator (CFI), Certified Incident Handler (CIH), as well as several certifications specific to products or companies, such as EnCase (EnCE), Cellebrite, and Microsoft. I am a Certified Information Privacy Professional (CIPP) and a non-active APICS certified professional in materials requirements planning and inventory management. I currently teach the applied Certified Ethical Hacker Course at the University of Minnesota and participate in Cyber Range exercises at Metro State University in St. Paul, Minnesota. In addition, I am an Executive in Residence at both Northern Illinois University and the University of Chicago. I am also an advisory board member of the Minnesota Academy of Science and Engineering.

8. During my 28 years of professional experience, I have held multiple positions in technology, technology leadership, and information security. My job roles have included: multi-country implementations of large enterprise resource

planning, customer relations management, and environmental resources management systems; artificial intelligence design using big data infrastructure; user interface and under experience design; global enterprise architectures; cloud architectures; cloud and on-premise infrastructure optimization; computer automated design implementations and configurations; and a variety of industry-specific technologies. I have performed both HIPAA (Health Insurance Portability and Accountability Act) and PCI DSS (Payment Card Industry Data Security Standards) security reviews, and am a non-active PCI-DSS Qualified Security Assessor, meaning I have been qualified by the PCI Security Standards Council to validate an entity's adherence to the PCI-DSS standard. In addition, I have managed one of just four groups hired by the U.S. Department of Health and Human Services, Centers for Medicare and Medicaid Services (CMS) to perform data validation and compliance reviews for over 25 U.S. health provider and payer organizations. In connection with this work, I testified at CMS in Baltimore and before the U.S. Senate Committee on Health, Education, Labor, and Pensions. I also have testified before the U.S. Senate regarding specific cyber security controls and standards required for compliance with the European Union's Data Directive and the U.S.-EU Safe Harbor Framework.

9. My cyber security knowledge spans the length of my years of professional experience. I have managed responses to major security incidents, performed information security investigations relevant to insider trading, credit card fraud, and social engineering attacks. I have conducted dark net investigations, packet-sniffing of mobile/cellular technology, offensive security projects, LAN/WAN/Wireless packet sniffing and analysis, vulnerability scanning, threat intelligence, forensics, penetration testing, cyber incident response, cyber incident remediation, incident handler roles, and cyber security attestation and audits.

10. I have been retained as an expert in 29 data breach actions. In this capacity, I have submitted numerous declarations, affidavits, and reports, and have testified at deposition and trial. I was a designated expert in the following matters:

- *Kleen Products, LLC v. Packaging Corporation of America*, No. 1:10-cv-05711-HDL (N.D. Ill.);
- *Andrew Giancola v Lincare Holdings Inc.*, No. 8:17-cv-02427-MHC (M.D. Fla.);
- *Fidelity Insurance Co. v. Express Scripts, Inc.*, No. 4:03-cv-1521-SNL (E.D. Mo.);

- *Schmidt et al., v. Facebook, Inc.*, No. C 18-05982 WHA (N.D. Cal.); and
- *Yahoo! Customer Data Security Breach*, No. 16-MD-02752-LHK (N.D. Cal.).

11. In this matter, I am being compensated purely on an hourly basis, plus actual expenses. My compensation is in no way dependent or contingent on my conclusions, opinions, or the outcome of the matter.

III. INFORMATION REVIEWED

12. Over the past 16 months, I have worked as an expert for Consumer Plaintiffs' Counsel in this matter. I have assisted Consumer Plaintiffs' Counsel on cyber security matters related to this case, including identifying the pre- and post-breach security controls in place at Equifax, how the data breach occurred, and the business practice changes that Equifax should implement in response to the data breach. In the course of the engagement, I have reviewed documents that Equifax and other parties produced in formal and informal discovery, listened to and reviewed testimony and interviews given by current and former Equifax officers and employees and information security personnel, and conducted independent research into Equifax's information security program. I have travelled to Atlanta to meet with and interview Equifax's information security personnel, and advised Consumer Plaintiffs'

Counsel as they negotiated the details of the business practice changes. All of these sources inform the opinions I provide in this Declaration.

IV. REVIEW AND EVALUATION OF BUSINESS PRACTICE CHANGES

13. From the information provided for my review during the litigation, it is clear that Equifax's pre-breach cyber security controls fell short of industry standards. This deficiency was amplified by Equifax's risk profile and the massive amounts of extremely sensitive consumer data that Equifax collected, processed, and stored.

14. If the Settlement Agreement is approved, the business practice changes required under the Settlement Agreement will improve Equifax's information security controls.

15. In the sections below, I provide a high-level explanation for some of the business practice changes included in the Settlement Agreement. In this Declaration, I do not attempt to discuss every business practice change or comprehensively analyze all of the cyber security benefits these changes will provide. Nonetheless, I believe the layperson's explanation I attempt to provide about the cyber security benefits of selected business practice changes amply illustrates the significant benefits these changes will provide to the Consumer Plaintiffs and the classes they seek to represent.

V. IMPLEMENT AND MAINTAIN A COMPREHENSIVE SECURITY PROGRAM

16. The Settlement Agreement requires Equifax to quickly implement, and then regularly review and revise a comprehensive information security program that is reasonably designed to protect the personal information that Equifax collects, processes, or stores on its network.[1]

17. This is a foundational information security requirement. As defined by NIST, a comprehensive written security program is an annually reviewed and executive-approved set of IT security policies, standards, control objectives, and guidelines. The security program is the entire collection of policies and procedures that govern the ability of an organization to protect the security, confidentiality, and integrity of the information it manages and includes all surrounding processes and infrastructure. The program's guiding principle is that it is easily implemented and auditable. Furthermore, NIST defines a comprehensive security program as one that also:

- Identifies and assigns roles and responsibilities among all organizational entities for managing the legal and regulatory compliance, confidentiality, integrity and availability of information assets;

[1] Term Sheet Ex. B, § 2.

- Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical);
- Contains the NIST required protocols such as standard security operating procedures, contacts, timelines, requirements, responsible parties, oversight and validation assessments;
- Is approved by executive management with ultimate responsibility and accountability for the risk incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals and other organizations;
- Encompasses the enterprise policies and procedures and incident response subprograms;
- Updates the plan to address organizational changes and problems resulting from security control assessments; and
- Protects the information security program and plan from unauthorized disclosure and modification.

18. My review of Equifax's pre-breach information security program revealed three key areas for improvement, each of which is addressed by this provision.

19. First, there were significant deficiencies in the substance of Equifax's pre-breach Information Security Program. On its face, this provision will require Equifax to fix those deficiencies.

20. Second, Equifax was slow to revise its pre-breach Information Security Program. For example, Equifax's security program did not include policies and procedures governing patching until 2015[2] and did not develop other key policies until 2016. These policies should have been in place much earlier, particularly for an organization like Equifax. By requiring Equifax to regularly review and revise its Information Security Program—and by mandating independent third-party assessments of those changes as discussed below—this provision will ensure that Equifax's Information Security Program adapts to addresses the changing cyber security landscape.

21. Finally, even where the policies contained within Equifax's pre-breach Information Security Program were adequate, Equifax did not always comply with its own policies and procedures. By requiring Equifax maintain a comprehensive and appropriate Information Security Program, and mandating that the independent third-party assessments evaluate both

[2] Staff of S. Comm. on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, How Equifax Neglected Cybersecruity and Suffered A Devastating Data Breach at 26 (available at https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf) ("Senate Report").

Equifax's "policies *and practices*,"[3] this provision will help ensure that Equifax's Information Security Program meaningfully protects PII.

VI. MANAGING CRITICAL ASSETS

22. The Settlement Agreement also requires Equifax to develop and maintain a comprehensive IT asset inventory.[4] This is a fundamental information security control that is typically included in a comprehensive security program.

23. At its core, an IT asset inventory is a constantly updated list of the IT assets that comprise a network, including computers, software, databases and data stores, switches, routers, firewalls, and other devices. The time-tested principle behind maintaining and systematically validating a comprehensive asset inventory is that an organization cannot maintain and protect what it does not know it has.

24. Maintaining an asset inventory with corresponding classification has been an industry standard for decades. NIST states, "The use of automated mechanisms to track the location of system components can increase the accuracy of component inventories. Such capability may also help organizations rapidly identify the location and responsible individuals of

[3] Term Sheet Ex. B, § 23(c) (emphasis added).
[4] *Id.* § 3.

system components that have been compromised, breached, or are otherwise in need of mitigation actions."[5]

25. Asset management provides the ability to measure utilization, centrally manage resources, and perform lifecycle and financial management. Most importantly, understanding what assets are allowed on a network or physically in a building provides for the ability to quickly identify, prevent, and/or eliminate unauthorized assets.

26. To effectively manage and classify assets, the inventory must also list other attributes for each asset. For example, the inventory must describe what, where, and how the asset is used and the types of information the asset accesses, stores, or processes. This lets the organization identify the appropriate privacy classification and criticality level of a given system and apply the appropriate information security and privacy policies and controls.

27. The IT asset inventory requirement is particularly important in the context of integrating acquired companies. Equifax has a documented history of acquiring companies with the potential for quick-to-market products and services and immediate revenue generation.[6] Integrating new systems and

[5] U.S. Dept of Comm., National Institute of Standards and Technology, Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, at 227 (available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf).

[6] Staff of H. Comm on Oversight and Government Reform, 115th Congr., The Equifax Data Breach (Dec. 2018) at 2 (available at https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf) ("House Report").

data into an existing network without a comprehensive understanding of the current network is a common way that acquiring companies make themselves vulnerable to cyber-attacks.

28. At the time of the data breach, Equifax did not have a comprehensive IT asset inventory. This directly contributed to Equifax's failure to patch the Apache server, which allowed the attackers access into Equifax's systems.

29. Accordingly, the Settlement Agreement's detailed provision for managing critical assets will help secure the information in Equifax's systems for the future.

VII. IMPLEMENT AND ENFORCE A DATA CLASSIFICATION AND HANDLING STANDARD

30. The Data Classification provision addresses some of the same concerns as the Managing Critical Assets provision discussed just above. This provision requires Equifax to maintain and update a data classification and handling standard, which also must be evaluated by the third-party assessors.[7]

31. In the context of data security and privacy, data classification provisions require the company to identity the types of data in its systems and assign a defined sensitivity level to each data type, usually based upon the sensitivity

[7] Term Sheet Ex. B, §§ 4 (Data Classification), 23 (Third-Party Assessments).

of the data (e.g., privacy concerns) and the level of impact to the company if the data were compromised. Once categorized, the company can apply the appropriate security, privacy, and handling controls to the data and related IT assets.

32. If proper asset management and data classification and handling had been in place at the time of the Equifax breach, all or nearly all of the data and assets in the dispute portal would have been categorized as highly classified and subject to increased monitoring and other security controls. Had this been in place, there is a strong likelihood the breach would have been stopped or detected before the data was exfiltrated.

VIII. LOGGING, MONITORING, SYSTEM INCIDENT AND EVENT MANAGEMENT

33. The Settlement Agreement provisions concerning Security Information and Event Management[8] and logging and monitoring[9] together require Equifax to implement security tools that will detect suspicious hacker activity so Equifax can repel the hackers before they are able to exfiltrate sensitive information. Equifax must remediate its pre-breach security deficiencies in this area and maintain and upgrade it its capabilities, under the oversight of the independent third-party assessor.

[8] *Id.* § 5.
[9] *Id.* § 6.

34. Security Information and Event Monitoring (SIEM) and other logging and monitoring processes and tools are akin to extremely sophisticated burglar alarms for computer networks. Put simply, logging and monitoring is the act of collecting and analyzing what happens on a computer system, comparing it to a baseline of normal behavior for the network, and alerting when pre-defined or anomalous behaviors are observed. When properly implemented, system activity will be automatically recorded in log files. A log may note, for example, that a particular user has accessed a system or that a user tried to use an incorrect password to log onto a database. The amount of log data collected generally increases with the sensitivity of the system. A SIEM is the common name for systems that mine vast quantities of real-time and historical log data for suspicious patterns of activity and issue a range of alerts based on that activity. Logging and monitoring and SIEM systems have been standard components of corporate information security programs for several years.

35. At the time of the data breach, Equifax had implemented some of these security controls in some parts of its network. In critical areas, however, these systems were never installed, had been misconfigured, or even disabled. Given the sensitivity of the information they stored, the breached portions of

Equifax's network should have been carefully monitored for intrusions, which would have led to the pre-breach detection of these hackers.

36. Stated simply, the Settlement Agreement requires Equifax to implement and correctly configure the processes and tools to log, monitor, and alert when anomalous behavior occurs. The provision contains the detail required to ensure meaningful security improvements, while providing Equifax flexibility to further improve security as technology changes of the course of the Settlement term. Furthermore, periodic third-party validation and testing to ensure the proper implementation and configuration will provide assurances that confidential data is being protected. These provisions are a critical security component that will allow Equifax to protect all consumer confidential data and the systems on which they reside.

IX. VULNERABILITY PLANNING, VULNERABILITY SCANNING, AND PATCH MANAGEMENT

37. The Settlement Agreement's provisions concerning vulnerability planning,[10] vulnerability scanning,[11] and patch management are complementary provisions designed to ensure that Equifax systematically anticipates, detects, assesses, and remediates vulnerabilities in the Equifax Network. In

[10] *Id.* § 9.
[11] *Id.* § 7.

this context, the term vulnerability simply means a potential information security weakness.

38. Vulnerability planning refers to an organization's overall strategy for identifying vulnerabilities, applying a risk categorization to each vulnerability, and remediating or eliminating the vulnerabilities on a timeline and in the manner appropriate for the risk category. It also includes processes for responding to third-party notices of proven or potential vulnerabilities. For example, when a vulnerability is ranked as "critical," the most severe rating, an organization should begin remediation planning within 24 hours and, if possible, complete remediation within one week. If remediation is impossible, then the company should instead implement appropriate compensating controls within that same week.

39. Vulnerability scanning is one process used to identify certain types of vulnerabilities. Vulnerability scanning tools search for known vulnerabilities one device, application, port, etc. at a time. The scan results should then be considered as part of the broader vulnerability planning and overall security program.

40. Patches are software updates that are released to fix bugs or address security vulnerabilities. Patch management is the administrative process of ensuring

that appropriate patches are implemented where they are needed and on an appropriate time frame.

41. The Equifax data breach is the textbook case for why vulnerability planning, vulnerability scanning, and patch management are vital components of an information system. Even before the Apache struts vulnerability exploited in this data breach was formally announced, online videos surfaced detailing how to take advantage of the Apache Struts vulnerability were available.[12] The videos had millions of hits and the step-by-step hacking process shown in the videos did not require advanced tech experience to perform. In addition, the actual scanning process to find out if a vulnerable Apache server was exposed to the Internet was free.

42. On March 8, 2017, the Apache Struts vulnerability was formally announced by the United States Computer Emergency Readiness Team. Two days later, unidentified individuals were scanning Equifax's systems for the vulnerability. Equifax did not ask system owners to install the patch that would fix the vulnerability until a week later. The vulnerability planning provision in the Settlement Agreement mandates a faster response.

43. Similarly, Equifax did not have an asset management system to identify all potential Apache servers, nor did it perform vulnerability scanning to find

[12] Senate Report at 34.

and validate that it had remediated all of its vulnerable systems, and therefore overlooked the unpatched server. The vulnerability scanning provision of the Settlement Agreement squarely addresses this issue.

44. Implementation of a comprehensive vulnerability planning and scanning process and tools would have mitigated, and most likely prevented, the Equifax data breach. Accordingly, these provisions provide important reassurances for the Class Members going forward.

X. FILE INTEGRITY MONITORING

45. Another important provision of the proposed business practice changes is the requirement that Equifax implement a governance process for file integrity monitoring.[13]

46. File integrity monitoring is a security control that involves detecting and alerting if security-relevant files on a system change unexpectedly or without authorization. While it is common for the files on a given system change to change, certain unauthorized changes can indicate that a cyber attack is underway. File integrity monitoring processes identify and isolate changes that are concerning and flag them for additional review. For example, hackers often disguise malware as a legitimate system file to avoid detection. By comparing the contents of such files to a known baseline, the file integrity

[13] Term Sheet Ex. B, § 13.

monitoring system can see through the disguise, delete the malware, and issue an appropriate alert.

47. File integrity monitoring has been a standard control in most comprehensive information security programs since 2012. Nonetheless, I was unable to find evidence of Equifax implementing file integrity monitoring on the breached dispute portal at the time of the breach, and publicly available sources indicate it was not in use.[14] Had file integrity monitoring been implemented on the dispute portal, it likely would have prevented the hackers from exfiltrating consumer data.

XIII. LEGACY SYSTEMS

48. Another key business practice change covered by the Settlement Agreement concerns remediating so-called legacy systems within five years of final settlement approval.[15]

49. In information technology parlance, a legacy system is an antiquated or outdated computer system that is still in use. Organizations sometimes obtain legacy systems through acquisitions. Alternatively, after long enough, the organization may have no employees who are sufficiently familiar with the outdated system to move the data onto a state-of-the-art system. Regardless of the reasoning, continued use of legacy systems often introduces many

[14] *See, e.g.*, Senate Report at 46.
[15] Term Sheet Ex. B, § 14.

security vulnerabilities, particularly because they often are not supported by their vendors.

50. At the time of the data breach, Equifax relied on a large number of legacy systems. Many of these systems were over 20 years old. Notably, the Automated Consumer Interview System (ACIS) that the hackers accessed was built in the 1970s. It is practically impossible to adequately secure data in a system of such antiquity. Nor was ACIS the only antiquated system in use at Equifax.

51. To address these vulnerabilities, the Settlement Agreement requires Equifax to fully remediate its legacy systems within five years of final settlement approval. Equifax also will be required to implement compensating controls to secure the systems pending remediation. Then, to ensure that Equifax does not continue to rely on legacy systems, the Settlement Agreement requires it to maintain an active lifecycle management process. This process will require Equifax to replace and deprecate legacy systems on an ongoing basis.

52. On its own, requiring Equifax to ending its reliance on legacy systems will substantially improve the security of Equifax's systems and the consumer information Equifax stores.

XI. MANDATORY TRAINING

53. The Settlement Agreement requires Equifax to provide at least annual training in information security to all employees, with additional training provided as appropriate based on the employees' job duties.[16]

54. Providing at least annual information security training to all employees is a standard component of an enterprise information security program and meaningfully reduces the likelihood that employees will fall prey to a phishing attack. Employees whose job duties require them to access sensitive information should augment the annual training with specific training that is appropriate for their job duties. Finally, even more specific training should be provided to employees working in information security.

55. In reviewing materials related to this case, I observed that the lack of adequately trained personnel was a factor that contributed to the data breach. Equifax had an information security training policy in place before the data breach, but no evidence the policy was followed. In addition, key personnel failed to fulfill their information security responsibilities. From this, I conclude that Equifax's pre-breach training program was inadequate. Because the types of training required will evolve over time, the Settlement Agreement permits Equifax wide latitude in designing a better training program for its employees. The sufficiency of that program, however, will be

[16] *Id.* § 18.

evaluated by the Third-Party Assessors, to ensure that the training is effective and appropriate.

XII. INFORMATION SECURITY SPENDING

56. To ensure that Equifax is able to complete the broad-ranging security upgrades required in the Settlement Agreement, the parties agreed that Equifax will spend at least $1 billion on data security and related technology over the next five years.[17] This represents a substantial increase over Equifax's pre-breach security spending. Further, in the course of my work, I have observed a pattern across many industries in which corporations provide ample funding to information security departments in the aftermath of a data breach. After a year or two, however, the companies drastically scale back information security funding, often before all of the planned security improvements have been completed. By requiring Equifax to spend at least $1 billion over five years, the Settlement Agreement aims to ensure that the business practice changes will be appropriately funded.

XIII. THIRD PARTY ASSESSMENTS

[17] *Id.* § 22.

57. The third-party assessment provision is the lynchpin of the business practice changes, and to my knowledge is more stringent than what has been obtained in any other private data breach settlement.[18] This provision requires Equifax to retain a qualified and unbiased cybersecurity organization approved by a regulator that will conduct rigorous assessments of its cyber security policies and practices, evaluate them consistent with established auditing procedures and information security standards, and establish deadlines for Equifax to shore up any deficiencies identified.

58. First, the organization conducting the Third-Party Assessment must be unbiased, independent, and qualified. To prevent any appearance of bias, the Third-Party Assessor must be approved by a regulator after Equifax discloses any compensated engagements with the Third-Party Assessor in the previous two years.[19] The provision also mandates that the Third-Party Assessor have appropriate qualifications and experience for the job.[20]

59. Second, the Third-Party Assessments will be procedurally rigorous. The assessor must either conduct an audit that meets the SOC 2 Type 2 attestation requirements or adhere to an industry-recognized auditing procedure that is approved by a regulator for use in the assessment.[21]

[18] *Id.* § 23.
[19] *Id.* § 23(a).
[20] *Id.*
[21] *Id.* § 23.

60. Third, the Third-Party Assessments will be substantively rigorous. The assessor is required to evaluate both Equifax's policies and its actual practices, and how they meet the requirements of NIST or a comparable cyber security standard.[22] And to the extent the specified business practice changes differ or exceed the applicable cyber security standard, the Third-Party Assessor also must confirm that Equifax has complied with the agreed-upon business practice changes.[23]

61. Fourth, the Third-Party Assessor has the authority to define the scope of the assessment.[24] This is a crucial requirement. Even the most wide-ranging cyber security assessment cannot examine every configuration setting on every system in a large corporate network. There is always some degree of sampling performed. In less rigorous assessments, the organization being audited chooses what the assessor examines—and they frequently avoid choosing vulnerable portions of their environments. In contrast, this Settlement Agreement gives the Third-Party Assessor sole authority to establish the scope of the assessment in consultation with Equifax.

62. Fifth, while it is common for cyber security assessments to identify vulnerabilities or areas for improvement, many companies are slow to fix the

[22] *Id.* § 23(c).
[23] *Id.* § 23(e).
[24] *Id.* § 23(b).

problems that are identified. The Settlement Agreement, however, requires the Third-Party Assessor to "establish dates by which Equifax shall remediate the deficiencies identified or implement compensating controls."[25] Thus, this provision is not merely a way to identify problems; it will drive their resolution.

63. As a final oversight measure, any material deficiencies identified by the Third-Party Assessor will be reported to Consumer Plaintiffs' Counsel along with the plan for remediating them.[26]

64. Altogether, this Third-Party Assessment provision is a real oversight mechanism that provides substantial benefits to consumers.

XIV. ADDITIONAL BUSINESS PRACTICE CHANGES

65. In addition to the business practice changes detailed above, the Settlement Agreement requires Equifax to develop and maintain information security controls in a number of key areas. These include penetration testing, threat management, access control and account management, encryption, data retention, vendor management, incident response exercises, treatment of data gathered through TrustedID, and breach notification.[27] Each of these controls

[25] *Id.* § 23(f)
[26] *Id.* § 23(g).
[27] *Id.* §§ 8, 11-12, 15-16, 19, and 20-21.

helps to safeguard the consumer information in Equifax's systems. But effectively implementing these controls will require Equifax to make many system-specific determinations, and the implementations may need to adapt over time as Equifax's security posture improves. To avoid freezing Equifax's security at current levels for the next five years, the Settlement Agreement requires that these controls be "reasonably designed" or "adequate." But because the Third-Party Assessments must evaluate settlement compliance, these provisions ensure that the Third-Party Assessors will make appropriate findings in light of security standards and risk postures at the time of the assessment. In my opinion, this managed flexibility improves the quality of the overall settlement for consumers.

SUMMARY AND CONCLUSION

66. In my assessment, comprehensive implementation of the proposed business practice changes should substantially reduce the likelihood that Equifax will suffer another data breach in the future. These changes address serious deficiencies in Equifax's information security environment. Had they been in place on or before 2017 per industry standards, it is unlikely the Equifax data breach would ever have been successful. These measures provide a substantial benefit to the Class Members that far exceeds what has been achieved in any similar settlements.

I declare under penalty of perjury, under the laws of the United States of America, that the above statements are true and correct.

Executed on this the 19th day of July, 2019, in Edina, Minnesota.

MARY T. FRANTZ

EXHIBIT A

MARY T. FRANTZ

5151 Edina Industrial Blvd
Suite 550
Edina, MN 554371

Office: (952) 496-2460
Mobile: (612) 239-5195
Maryf@ekpartner.com

Professional Summary

- Both full time and interim executive leadership roles in technology, security and operations for Fortune 100 and multiple start-ups; Lead teams in excess of 300, managed a successful business for 15 years' with over 17 full time consultants and more than 35 subcontractors.
- IT Security and Audit experience and certifications including CISA, CIPv3/5, CEH v7/9, CPT, CMS / HHS Data Validation certified auditor, CIPP, HITRUST, FINRA, Sarbanes-Oxley, HIPAA / HITECH, CMS, GLBA, PCI, CFR Part 11, Basel III, ISO 27002, SSAE16/18, GDPR, FedRAMP, NYCRR 500, and CMS Data Validations.
- Expert witness in 12 national data breach investigation and litigation cases; primary expert in over 19 data breach (including EU data directive sanctions) investigations, 27 corporate investigations including but not limited to IP theft, contract disputes, data analysis, medical/healthcare fraud, financial compliance, insider trading and foreign corrupt practices (FCPA).
- As a senior executive consultant with two major energy companies; provide input into the smart grid privacy, security and rate case reviews.
- Provided expert testimony and deposed in cyber security incidents, CMS data validations for health care issues and fraud, financial issues, telecommunication, voice/data / telemetric implementations, investigations, data/call/billing detail and VOIP.
- Over 20 years' experience working with in health payer, provider, device and pharma organizations.
- Experienced executive leader (Director and Officer); interim CIO, CISO, and CCO (Chief Compliance Officer) for several clients.
- Designed the CMS federal data validation audit template and lead audits on over 25 health plans nationwide.
- Performed and / or lead the forensic investigations, extractions, review and production in over 30 national and international cases.
- Lead multiple distinct global ERP / CRM / EMR implementations at Fortune 500 firms over 15 years (Oracle, JDE, SAP, Exact, Sage, EPIC, McKesson, Cerner, Infor, Lawson, and others).
- Fluent in design, development of cloud and virtual systems.
- Lead and participated in over 15 process design improvements and reengineering for global energy and manufacturing organizations.
- Designed and implemented IDM / IAM solutions in multiple organizations and part of he original IDM architecture at Novell, Microsoft and Cisco.
- Extensive business process re-design at all corporate levels with proven savings in excess of $20M
- Aggregate project savings in excess of $25M through strategic consolidations, architecture and development methodology alignment
- Paneled executive round-table discussions, taught over 7 CLEs on eDiscovery, Legal Hold, Cybersecurity, Data Breach prevention and currently one of the few non-attorney leaders requested to contribute and lead subsections on the MN e-Discovery Working Group and Civil Task Report on improving eDiscovery and forensic technology processes for the State and Federal Judiciary
- Fluent in engineering platforms, manufacturing systems, telecommunications, and other environments, non-active APICS certified
- Multi-lingual with extensive multinational experience

Professional Experience

ENTERPRISE KNOWLEDGE PARTNERS, LLC, (2004 - Present), Founder and Managing Partner

Founded EKP, LLC in 2004. Mary is a keynote speaker, publisher, and quoted in over 10 technology and industry journals. EKP is vendor agnostic and will not act as a reseller in any capacity.

Services offered:

Technology Strategy

- Enterprise Architecture and Infrastructure
- Technology Strategy & Alignment
- M&A Consolidations, Data Mapping
- ERM, Claims, ERP (SAP, Oracle, Lawson, Facets, Epic, Infor, Exact, and more)
- Testified on identity management systems and health care claims adjudication, Managed Care Benefit Utilization statistical calculations, RICO, ERISA
- Big Data (Hadoop frameworks, Mongo, Cassandra, Hive and more)

Security / Incident Response:

- Breach Remediation
- Vulnerability Scanning, Penetration Testing
- IR/DC/BC Strategy and Testing
- Internal Investigations
- Expert Testimony (variety of cases)

Forensics:

- Collection: Onsite and Remote
- Computer, Network, Cloud, Mobile, Specialty Products
- Fraud Detection
- Internal Investigations
- Expert Testimony (variety of cases)

Audit / Compliance

- Security and Privacy policy frameworks
- FISMA, NIST CSF, HIPAA Security, CSA, OCC, Sarbanes Oxley, FedRAMP, SSAE16/18
- Specialists in Safe Harbor / GDPR
- Security / Privacy / Risk Posture Assessments / PIA
- Security Architecture, Design
- IT Risk Management and Controls

- **Clients:** Current and past clients include, but not limited to: Imagine! Print Solutions, Mayo Clinic, Hewlett Packard, Zimmer Medical, MaxMind, Patterson Companies, Compeer Financial, Amplifon, MedNet, Glen Eagle Financial Advisors, Cabela's, John Deere, Office Depot/Office Max, Carlson Companies, Allianz Life, Novartis, International Truck, CH Robinson, Starkey Labs, ATS Medical, St. Jude Medical, Nystrom, US Department of Homeland Security, US Department of Defense, US Center for Medicare and Medicaid (CMS), US Department of Health and Human Services (HHS), Fairview Health Services, Select Comfort, Post Foods, Gander Mountain, HeathEast Care Systems, Sanford Health, Prime Therapeutics, WellPoint, Anthem, Uromedica, Xcel Energy, United Bankers

Bank, Exxon, Sunoco, Johns Hopkins, Herman Gerel, LLP, Seyfarth Shaw, LLP, Winthrop & Weinstein, Lockridge Grindal Naun, Mendoza Law, Skadden, Weitz & Luxemberg, Stohl Rives, Littler Mendelson, Briggs & Morgan, Principal Financial, Delta Dental of MI/IN/OH/NC, Blue Cross / Blue Shield organizations (25), State of Illinois Department of Insurance, Minnesota State Court Administration, Minnesota Judicial Department, Washington County, Shutterfly, Pentair, Whirlpool Corporation, McGough Construction, Delta Dental, MedNet Study, HP, Google, Goodwin Proctor, Verata Health, Health, Seeger & Weiss, various other national law firms and corporations

- **Client Leadership Roles:** Interim Director of IT; CSO / CISO, Chief Compliance Officer, Chief Privacy Officer, Interim Chief Information Officer, Interim Board Member; Acting Sr. Business Strategy Manager; Senior Program / Project Manager; Sr. eDiscovery Advisor; and Chief Auditor
- **Speaking Engagements:** Computer Enterprise and Investigations Conference (CEIC), Upper Midwest Employment Law Institute , Twin Cities Privacy Retreat, IQPC eDiscovery for Financial Services (NY and DC), ARMA (Dallas, Chicago, and Minneapolis), Financial Executives International (FEI), Midwest Society of Association Executives (MSAE), Cyber Security Summit, Secure 360, Women in eDiscovery (WIE), Forbes CIO Retreat, Health Information Management Systems Society (HIMSS), guest lecturer at NYU Law School and Cardozo School of Law (NY) for both e-Discovery and Health Law topics, Cardinal Stritch Marketing and Business Communications lecturer, Northern Illinois University, StemCONNECTOR, ACC (Association of Corporate Counsel), University of Minnesota, University of Chicago, Enterprising Women International Conferences (Cape Town, SA, Lisbon, and Miami FL), eClub International, Cyber Security Summit, RSA, Federal Bar Association, 2018 UBB National Conference, 2018 MN IT Government Symposium
- **Lecture/Education:** Guest Instructor University of Minnesota Humphrey School of Law – eDiscovery and Forensic Seminar; University of Minnesota, St. Paul and Metro State, St. Paul - Security and Ethical Hacking; Guest Lecture University of Chicago and Northern Illinois University: Master's in Information Systems Lecture on Information Governance; MNCaps Corporate Sponsor, Student Mentor in Business Pathways, Guest Expert Capstone Projects Anoka Hennepin School District (Jackson Middle School), Guest Instructor University of Virginia and University of Virginia Law School.

CARLSON MARKETING GROUP, INC., Plymouth, MN **July 2003 – May 2004**

Sr. Director, Architecture & Security Services: Responsible for IT applications architecture, security and audit compliance, privacy, litigation support, application development and IT service marketing strategy for both internal and external customers. Customers included US Government Travel Office, Merck, Visa, Target Corp., Northwest Airlines, British Airways, Certegy, State Farm Insurance, MBNA, Bates Casket Co., Hewlett Packard, and Hallmark.

- Achieved eight commendations for innovative leadership
- Developed the common architecture and security framework for marketing to external customers
- Created defensible practices and responsible for contract drafting oversight and contract audit
- Implemented enterprise IDM solution
- Led and managed matrix teams throughout IT and Operations to perform the following:
  - An enterprise service-oriented architecture and identity management strategy
  - Infrastructure (server /mainframe, and network capacity) planning strategy and implementation
  - Enterprise business architecture strategy planning, including marketing and sales organizational structure
  - Development of product and service pricing strategies; sales presentations and RFP responses
  - Developed two-year strategy plan for compliance with SOX, HIPAA, Visa CISP / MC DSP and ISO17799
  - Primary representative for litigation support and eDiscovery for corporate systems

CONSULTANT **June 2001 – July 2003**
Hired on retainer or hourly for multiple roles:

- Lead eDiscovery of email; help desk and eCommerce systems for Land O'Lakes v Farmland Feed.
- Created successful bid for large corporate partnership agreement on behalf of two local consulting companies for Data Warehouse / CRM implementation and Oracle 11i upgrade.
- Assessment and merger recommendations; due diligence
- New business venture development assessments
- RFP and proposal project management
- Applications Architecture Strategy and Business Process Assessment for medium sized medical manufacturing firm; resulted in operational savings in excess of $1M annually after expenses (Centerpulse / SpineTec).
- Integration of Purina Mills and Terra Industries for Land O Lakes with subsequent relocation and closing of farm animal feed locations; simultaneous management of 119 networked co-op locations throughout the US for feed and seed
- JDE, Oracle, PeopleSoft, SAP conversions and implementations

ORION CONSULTING, INC., Bloomington, MN **October 2000 - June 2001**

ERP, Compliance Technology and Operations Strategy Practice Lead
Overall responsibilities included directing the individual consulting industry verticals in strategic assessments primarily based on technological support of business strategy objectives for world-wide client base.

- Formulated proposals, client presentations and advising on strategic directions for business functional and technical teams
- Contracted team for large defense manufacturing organization to develop long term business and technology strategy
- Developed BPA strategy for realignment within Oracle 11i applications (improved use of BOM, Inventory, and eProcurement modules; implementation of VAT tax systems, GL consolidations of multi-org environments
- Managed and developed industry partnerships in the CRM, ERP (Oracle), and the B2B/C software applications practices.
- Authored white papers on CRM, Knowledge Management, and Identity Management

NOVELL, INC., Provo, UT / San Jose, CA **November 1997 – September 2000**

Sr. Director, Global e-Business Engineering New Product Management & Architecture:
Senior director of global IT architecture and identity management product engineering for 5 countries. Business duties included promoting security products and congressional lobbying for tools designed to reduce identity theft, lobbying for EU recognized safe harbor provisions, and other security and privacy considerations. Internally, responsible for business engineering product/project management regarding all enterprise applications including Oracle ERP and Seibel, PeopleSoft, VAT taxing in EMEA, and ecommerce "bolt-ons" for Novell's ASP / ISP presence for channel on-line sales, outsourcing retail sales distribution and product warehousing, IDM zero-day start. In addition, achieved proven operational savings exceeding $2.5M. External clients included, but not limited to, Hewlett Packard, Oracle, Republic of Germany (country), CNN, US Airforce, and 3M. Performed expert witness testimony in multiple lawsuits.

Global Program Director, ITS Applications Architecture:
Responsible for global teams in 5 countries implementing and managing global data warehousing and web portal solutions (Cognos, Brio, Microstrategies, and Hyperion); Enterprise project/program management guidelines / governance; implemented collections system for Finance; ISO 9000 certification; all

manufacturing systems of gold master CD's and related global distribution of product via online sales and distributers.

Manager, Business Applications and New Technology:
Developed hardware specifications and budget for strategic 3-year implementation plans and provided technical consultation with executive level customers explaining business values of technical decisions and computing ROI. Direct reports consisted of 45 contractors and 12 Novell senior developers. Managed employees in the Dublin (Ireland), San Jose (CA), and Orem/Provo (UT) offices.

Manager, Global Financial Applications:
Management of all business financial application services for Novell in 7 different countries including contract management and sales tools.

TOTAL SYSTEMS SERVICES, Columbus, GA / Global February 1996 – June 1997

Product Manager / Assistant VP, Total Access:
Ms. Frantz created the Total Access SAS team providing on-site consulting services for portfolio and custom credit analysis applications. Customers included but not limited to GECF, GE Fleet, Banjercito, Banco Central de Mexico, Royal Bank of Canada, Peoples Bank, Bank of America, Federal Reserve of Chicago and Minneapolis, Nations Bank, and Wells Fargo. Overall quarterly net revenue generation exceeded $1M in consulting services / licensing fees, and $800K in custom package development. In addition, Mary provided language translation for South and Central American customers and worked with international partners to monitor and prevent credit card and banking fraud.

FMC / MCI TELECOMMUNICATIONS, Atlanta, GA / Dallas TX May 1991 – February 1996

MCI Team Lead/Project Lead Corporate Business Engineering, Atlanta GA
Overall responsibility for customer-based and MCI enterprise projects for large corporate voice and data accounts.

MCI Team Lead: Sr. Systems Analyst, Atlanta, GA
Awarded small business Director's Club award three consecutive quarters for highest performing team.
Team was responsible for managing the outsourced Microsoft call center systems and analyzing voice and data line minutes and revenue for small business services division.

FMC Consultant / Project Team Lead, Dallas, TX
Managed resource measurement analysts team including production conversion of MVS 3.3 to MVS 4.2; conversion from Pace Kommand Chargeback systems to MICS Accounting and Chargeback; upgrade from SAS 5.18 to SAS 6.07. Resource measurement for all defense and navel R&D and manufacturing facilities, FMC Gold, Food Manufacturing (FMG) and Airline Equipment divisions (AED). Analyzed and testified for the Tariff 12 AT&T agreement on behalf of FMC, US Senate hearings

FMC Resource Measurement Analyst, San Jose CA and Dallas TX
Responsible for primary support and maintenance for internal and external customer chargeback systems on all platforms and Capacity planning on four platforms including voice and data primarily to support Gulf War activities including Telco fraud investigations, system security and contract base-lining for Department of Defense, foreign language translation of project requirements for international customers.

Education & Professional Certifications

Education / Honors:

Minnesota Academy of Science and Engineering
- Lead Judge State Science and Engineering Fair for MS and HS– Technology, Physics and Ecology (2014 – present)

STEMConnector
- Top 100 Leaders in STEM 2016

Enterprising Women Magazine
- 2016 Enterprising Woman of the Year
- 2017 Foundation Award Winner

Northern Illinois University – Appointed Executive In-Resident
- MIS Experiential Learning Center for MIS candidates

Business Journal – Twin Cities
- 2008 Top 25 Women to Watch

National Organization for Women Business Owners – National and MN Chapter
- 2007 Young Business Woman of the Year

National Organization for Women Business Owners – MN Chapter
- 2005 Recipient of the "Woman on the Way"

Bachelor of Science 1991 – Northern Illinois University, Dekalb, IL
- Concentration: Information Systems and Operations Management

Bachelor of Science 1991 – Northern Illinois University, Dekalb, IL
- Concentration: International Relations

Bachelor of Arts 1991 – Northern Illinois University, Dekalb, IL
- Concentration: Foreign Language Business Translation (Spanish & French)

Bachelor of Arts 1991 – Northern Illinois University, Dekalb, IL
- Concentration: Math / Statistics

MBA, University of Chicago
- Concentration: International Business/International Finance and Investment

MS, Georgia Institute of Technology, Atlanta, GA and University of Texas at Arlington
- Maters of Engineering - Computer Science Engineering

Activities, Boards, Memberships & Certifications

- MN Cyber Range – Instructor via Metro State College
- Certified Ethical Hacking Adjunct Professor – University of Minnesota
- Board Director, Minnesota Academy of Science, Minnesota Academy of Applied Sciences - Treasurer
- Advisory Board, Enterprising Women International and Enterprising Woman Magazine
- Advisory Board, Cyber Security Summit
- Elected School Board Director – Prior Lake / Savage District 719 (2016 – present)
- SouthWest Metro Intermediate District – Board of Directors
- Adjunct/Guest Expert, Mayo Clinic - Board of Trustees
- Association for Records Management (ARMA) - chapters in MN, Chicago, and Dallas
- Millennial Leaders, Upper Midwest Chapter
- Women in e-Discovery, Lead Sponsor, Twin Cities

- APICS – Chicago chapter, non-active certification in Inventory and MRP II
- National Organization for Women Business Owners (NAWBO)
- Information Systems Audit and Control Association (ISACA)
- Performance Measurement Association (PMA)
- International Standards Organization (ISO) - contributing member
- Enterprise Architecture Community (EA)
- HITRUST CSF
- CISSP Certified Information Systems Security Professional
- CISA Certified Information Systems Auditor 2007, recertified June 2012
- CEH Certified Ethical Hacker certified 2009, re-certified March 2013 CEHv7, CEHv9, CEHv10
- CPT Certified Penetration Tester (InfoSec Institute)
- CIPP Certified Privacy Professional – US and EU (EU is non-active, waiting re-cert test)

REFERENCES and LEGAL MATTERS AVAILABLE UPON REQUEST